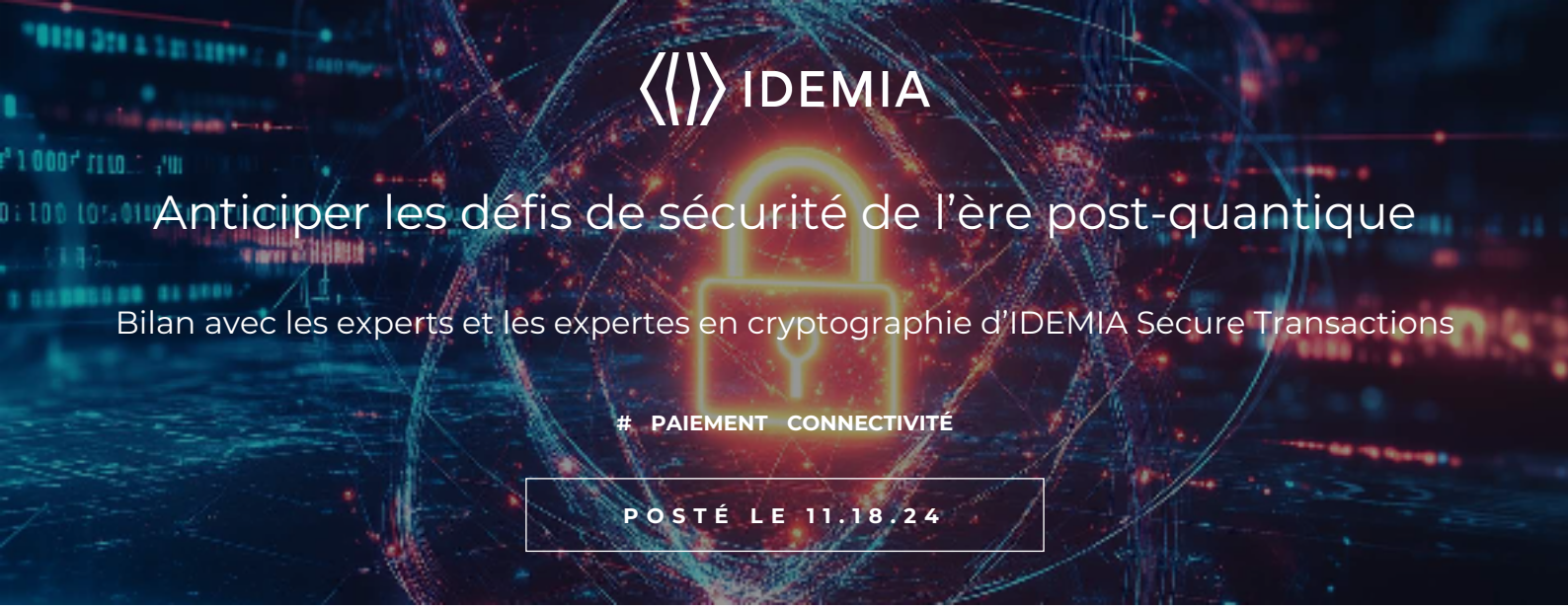

Anticiper les défis de sécurité de l'ère post-quantique

Bilan avec les experts et les expertes en cryptographie d'IDEMIA Secure Transactions

PAIEMENT CONNECTIVITÉ

POSTÉ LE 11.18.24

En quelques années seulement, les ordinateurs quantiques sont devenus ce qui pourrait être l'une des technologies les plus transformatrices des années à venir. Les technologies quantiques sont extrêmement prometteuses pour un grand nombre d'industries. Dans le domaine de la cryptographie, l'un des fondements de la sécurité qui se trouve au cœur des produits et des systèmes que nous utilisons tous les jours, l'émergence de ces technologies vient rebattre les cartes. Entre risques et opportunités, les experts et les expertes en la matière s'y préparent depuis des années. Voici un point sur la situation à l'heure actuelle et leurs conseils face à ce défi sans précédent.

Ordinateurs quantiques : une dynamique de développement et d'industrialisation qui s'accélère

En permettant de résoudre des problèmes jusqu'alors insolubles avec les ordinateurs conventionnels les plus puissants à l'heure actuelle, les ordinateurs quantiques sont porteurs de nombreux espoirs. Bientôt, ils devraient permettre de découvrir de nouveaux matériaux, de synthétiser de nouveaux composants pharmaceutiques, ou d'optimiser la logistique, les réseaux télécoms et les infrastructures électriques. Ils devraient aussi aider à réduire drastiquement les ressources nécessaires pour les calculs de plus en plus complexes effectués par les outils d'intelligence artificielle, qui, déjà à l'heure actuelle, poussent dans leurs retranchements les plus grandes infrastructure Cloud (dont on pensait pourtant les ressources inépuisables).

A mesure que sont identifiées les applications concrètes que peuvent avoir les ordinateurs quantiques, la communauté quantique s'élargie et les investissements augmentent rapidement. D'après une étude réalisée par PwC en 2023 sur les technologies émergentes, 29% des CEOs envisageaient déjà d'investir en priorité dans les technologies quantiques en 2024[1]. De nombreux secteurs espèrent que les ordinateurs quantiques pourront bientôt devenir une réalité industrielle grâce aux percées scientifiques et techniques actuelles et à ces investissements croissants, même si nul ne peut vraiment prédire dans combien de temps, ni quelles seront réellement leurs capacités.

L'intérêt majeur des ordinateurs quantiques réside dans leur capacité à réaliser certains calculs à une vitesse incomparable par rapport à celle des ordinateurs actuels. Cela sera très utile dans certains domaines mais cela comporte aussi un risque : à moyen ou long terme, en viendront-ils ainsi à donner les moyens à des acteurs malintentionnés de casser les algorithmes et les protocoles de sécurité auxquels nous faisons confiance depuis des décennies ? Impossible de déterminer avec certitude l'ampleur de l'impact que les ordinateurs quantiques pourraient avoir sur les systèmes de sécurité actuels, mais aussi hypothétique soit ce risque, une chose est sûre : nos sociétés ne peuvent absolument pas se permettre de le prendre.

Cette accélération des investissements et des avancées techniques dans le domaine quantique, sur fond d'enjeux croissants de souveraineté et de cybersécurité à l'échelle internationale, créé une réelle situation d'urgence pour tous les acteurs de la sécurité à travers le monde.

Paul Dischamp, Cryptography Lab Director chez IDEMIA Secure Transactions

La sécurité post-quantique : un enjeu actuel

On aurait tort de penser que le risque est encore loin. La menace que font planner les avancées des technologies quantiques sur la cryptographie qui protège aujourd'hui nos données et nos transactions est déjà une réalité. Les professionnels de la sécurité ne peuvent pas rester sans réagir face à cette menace. Trouver la parade est une responsabilité pour tous les acteurs de l'industrie de la sécurité.

Depuis des années, nombreux sont ceux qui se sont retroussé les manches à travers le monde et qui, fort heureusement, n'ont pas attendu que la menace quantique fasse les gros titres pour prendre la mesure des enjeux. IDEMIA Secure Transactions en fait partie.
Le risque le plus imminent est la stratégie d'attaque qui consiste à "collecter maintenant et déchiffrer plus tard" des données chiffrées, c'est-à-dire à les stocker en attendant d'avoir accès à la puissance de l'ordinateur quantique pour les déchiffrer. Un autre risque, auquel on pense peut-être moins spontanément, est celui lié aux milliards d'objets connectés constituant l'Internet des Objets et dont la durée de vie peut aller jusqu'à 15 ou 20 ans (voitures connectées, compteurs intelligents, terminaux de paiement, etc.). Si des ordinateurs quantiques capables de casser les cryptosystèmes actuels voient le jour alors que ces appareils sont encore en service, leur sécurité sera grandement compromise.

Les fournisseurs de services critiques doivent commencer la migration vers la cryptographie post-quantique dès maintenant, car la transition d'un écosystème entier vers de nouvelles technologies est un processus qui prend du temps. Ce ne sont pas seulement les algorithmes qui doivent être mis à jour, les protocoles et différents appareils doivent également être adaptés. Plus vite cette migration sera menée à bien, plus vite la sécurité à long terme des infrastructures sera assurée.

Christophe Giraud, Cryptography & Product Security Group Manager chez IDEMIA Secure Transactions

Agilité : être prêts à n'être jamais complètement prêts face à l'ordinateur quantique

Peu de temps après avoir atteint le dernier tour de sélection dans la compétition lancée par le NIST (National Institute of Standards and Technology) en 2016 pour la standardisation de nouveaux modèles cryptographiques résistants à l'ordinateur quantique, l'un des premiers modèles candidats était mis en défaut, non pas par un ordinateur quantique mais par un ordinateur conventionnel. Rien de surprenant à cela pour les experts et les expertes en cryptographie, c'est le processus normal : un examen rigoureux et une analyse continue sont essentiels pour confirmer (ou réfuter) la robustesse d'une solution cryptographique.

Cet exemple est révélateur du fait que la « menace quantique » ne doit pas faire baisser la garde face aux moyens déjà à la portée des attaquants et démontre aussi le degré d'incertitude quant à la robustesse de tout nouvel algorithme cryptographique vis-à-vis des menaces actuelles et à venir.

La confiance dans les algorithmes et les solutions cryptographiques que nous utilisons actuellement ne s'est pas établie du jour au lendemain. Pareillement, même si nous avons déjà un bon niveau de confiance dans les algorithmes et les protocoles de cryptographie post-quantique qui viennent d'être standardisés, il faudra une dizaine, voire une vingtaine d'années pour vraiment s'assurer de leur robustesse. Il est normal de faire évoluer les choses progressivement pour assurer la sécurité à long terme.

Emmanuelle Dottax, Cryptography Architect chez IDEMIA Secure Transactions

Le nécessaire temps de maturation des technologies de cryptographie post-quantique est un paramètre qui a été pris en compte dès le départ par les experts et les expertes qui ont ouvert ce nouveau champ de recherche. C'est la raison pour laquelle les principales institutions chargées de définir les normes de sécurité préconisent une approche hybride qui consiste à coupler cryptographie classique et cryptographie post-quantique. Autrement dit, plutôt que de remplacer l'ancien cadenas (la cryptographie classique), par un nouveau (la cryptographie post-quantique) mieux vaut ajouter le second au premier.

A mesure de l'évolution des nouveaux standards de cryptographie post-quantique, la crypto-agilité, qui consiste à pouvoir changer à distance tout ou partie d'une solution cryptographique déjà déployée sur le terrain, fait également partie des prérequis. C'est la clé pour pouvoir réactualiser les défenses en temps réel, dès la découverte d'une vulnérabilité, sans mettre à l'arrêt les systèmes ou sans avoir à rappeler tous les appareils équipés d'une puce. Cette approche proactive permet de s'adapter et d'assurer la sécurité en continu, avec des systèmes résilients et qui restent à jour.

Se préparer à la sécurité post-quantique implique de faire preuve de flexibilité dès maintenant, afin d'être prêts à faire des mises à jour et à relever les défis futurs de façon transparente. Au fil de l'évolution des standards cryptographiques, la crypto-agilité sera essentielle pour maintenir la confiance dans les systèmes de sécurité.

Luk Bettale, Cryptography Group Manager chez IDEMIA Secure Transactions

Si dans un environnement très flexible et connecté (comme un serveur), ce type de mise à niveau ne présentera pas réellement de difficultés techniques, il s'agira d'une opération bien plus délicate dans des environnements aux ressources et à la connectivité limitées tel que l'élément sécurisé d'une carte à puce. C'est pourquoi les spécialistes de la conception de puce et du développement d'OS sécurisés d'IDEMIA Secure Transactions sont à pied d'œuvre pour définir des produits à l'architecture la plus flexible possible et pour y intégrer les dernières fonctionnalités de sécurité qui permettront de protéger ces opérations particulièrement sensibles.

Préparatifs : standardisation des nouveaux algorithmes cryptographiques

Tout récemment (en août 2024), après 8 années de recherches et d'évaluations, un premier jeu de standards s'appuyant sur 3 algorithmes (l'un pour l'établissement de clés, les deux autres pour les signatures numériques) vient d'être finalisé par le NIST. Tout en continuant à étudier d'autres algorithmes pour renforcer et compléter cette première ligne de défense, l'organisation appelle déjà toute la communauté informatique à implémenter sans tarder les premiers standards.[2]

En parallèle de sa contribution active à la recherche et aux efforts de standardisation du NIST, IDEMIA Secure Transactions progresse déjà en ce qui concerne le déploiement des premiers standards disponibles, ce qui n'est pas aussi simple qu'on pourrait le penser. En pratique, pour que ces nouvelles défenses post-quantiques deviennent une réalité, l'un des enjeux est l'efficacité des implémentations. Tout l'art est de réaliser celles-ci de la bonne manière, c'est-à-dire en tenant compte des cas d'usage et des spécificités de chaque environnement.

Les nouveaux algorithmes standardisés par le NIST n'ont pas été initialement conçus pour les systèmes embarqués, lesquels imposent des contraintes spécifiques. L'une des priorités est de rendre les implémentations des algorithmes post-quantiques résistantes face aux attaques par canaux auxiliaires et par injection de fautes auxquelles les systèmes embarqués sont particulièrement exposés. Les techniques d'implémentation permettant de sécuriser les algorithmes classiques ne sont pas toujours adaptées aux algorithmes post-quantiques. Il faut donc trouver de nouvelles méthodes pour les protéger. Il s'agit parfois d'un véritable défi, mais c'est absolument essentiel. Aguerrie en la matière, l'équipe cryptographie d'IDEMIA Secure Transactions contribue activement à l'élaboration de ces nouvelles méthodes. Cela a déjà fait l'objet de plusieurs publications lors de conférences de premier plan dans le domaine de la cryptographie embarquée, avec une attention particulière portée à l'implémentation des algorithmes sélectionnés par le NIST (ML-DSA, ML-KEM).[3]

A ces spécificités en matière de sécurité, s'ajoutent des défis liés à la puissance de calcul et à l'espace mémoire intrinsèquement limités des éléments sécurisés. Les protocoles post-quantiques doivent être conçus de façon à maintenir le même niveau de fonctionnalité qu'avec la cryptographie classique, malgré ce niveau de contrainte très élevé. Par exemple, lors de la 5e conférence de standardisation post-quantique organisée cette année par le NIST, l'une des doctorantes d'IDEMIA Secure Transactions a présenté une technique pour optimiser le processus de génération de clés pour des signatures numériques dans un environnement embarqué.[4]

> *Au-delà de la recherche d'algorithmes cryptographiques capables, en théorie, de résister à la puissance de calcul des ordinateurs quantiques, il est également essentiel de s'assurer que leurs implémentations allient sécurité et optimisation des performances pour des applications concrètes.*
>
> Rina Zeitoun, Cryptography Engineer chez IDEMIA Secure Transactions

Vision d'ensemble : de la théorie aux applications concrètes de la cryptographie post-quantique

Sur tous les fronts, les experts et les expertes d'IDEMIA Secure Transactions n'ont de cesse de mettre en œuvre les premières défenses post-quantiques sur le terrain. La mission est de taille : protéger les identifiants, assurer l'intégrité des données, garantir la fiabilité et la confidentialité des transactions mais aussi préserver la vie privée des utilisateurs et prévenir les failles de sécurité qui mettraient à mal la réputation d'entreprises qui fournissent des services essentiels partout dans le monde.

> *Le défi de la cryptographie post-quantique ne connait pas de frontières, tous les pays doivent se préparer à l'avènement de l'ordinateur quantique. En parallèle de nos contributions aux efforts de standardisation pilotés par le NIST depuis les Etats-Unis, nous nous engageons pour faire progresser la cryptographie post-quantique à travers le monde.*
>
> Marc Bertin, Chief Technology Officer d'IDEMIA Secure Transactions

S'assurer des performances des modèles de cryptographie post-quantique en conditions réelles implique les efforts coordonnés de nombreux acteurs de la chaine de sécurité. C'est pourquoi IDEMIA Secure Transactions travaille conjointement avec les agences de sécurité mais aussi avec ses clients, avec d'autres acteurs de la sécurité et avec des start-ups pour tester des cas d'applications concrets.

Les preuves de concepts d'IDEMIA Secure Transactions sont axées autour de deux priorités clés : protéger les données contre les menaces du type « récolter maintenant, décrypter plus tard », et aider ses clients et partenaires à préparer la migration post-quantique, avec une approche globale de l'écosystème.

Assurer la protection des données grâce à des solutions de chiffrement avancé est au cœur de l'expertise de l'entreprise. Début 2019, IDEMIA a été l'une des premières entreprises à annoncer le développement d'une carte à puce résistante aux ordinateurs quantiques. Deux ans plus tard, en prévision des nouvelles normes ETSI et GSMA, IDEMIA Secure Transactions testait déjà de façon proactive l'intégration des premiers algorithmes post-quantiques dans ses SIM 5G Quantum-Safe avec Telefónica España pour protéger la vie privée des abonnés. Plus récemment, IDEMIA Secure Transactions a également testé avec succès la protection de données en transit vers un appareil IoT en utilisant la première connexion TLS (*Transport Layer Security*) résistante à l'ordinateur quantique en s'appuyant sur une eSIM crypto-agile.

A la tête du consortium Hyperform financé par France 2030 et l'Union européenne, IDEMIA Secure Transactions travaille également sur la protection en profondeur des données contre les menaces quantiques au-delà de ses activités traditionnelles, aux côtés d'autres leaders français de la cybersécurité. Ce consortium étudie la protection des données de bout en bout pour des écosystèmes informatiques complexes (stockage de données dans le cloud, archivage de documents et collaboration en ligne), en utilisant les capacités de crypto-agilité d'une carte à puce pour maintenir la sécurité post-quantique dans le temps.

> *La cryptographie est partout, et elle est au cœur de notre métier. Nous avons énormément à faire pour identifier et étudier tous les cas d'applications de la cryptographie post-quantique. Cela nécessite l'implication de tout l'écosystème de la sécurité, mais aussi des mises en pratique en conditions réelles, en étroite collaboration avec nos clients.*
>
> Olivier Nora, Chief Open Innovation chez IDEMIA Secure Transactions

En tant qu'entreprise précurseuse de la migration quantique au sein de l'écosystème mondial, IDEMIA Secure Transactions est activement impliquée dans la migration des appareils edge connectés aux services digitaux (c'est à dire les appareils qui se trouvent être les points d'extrémité des réseaux dont ils font partie) : cartes de paiement, véhicules, appareils IoT tels que les compteurs intelligents… Cette migration devra avoir lieu avant que les ordinateurs quantiques ne disposent de capacités suffisantes pour casser la cryptographie classique. Elle doit être anticipée le plus tôt possible. En s'associant avec des instituts de recherche, des fournisseurs de solutions et ses clients pour réaliser des implémentations de bout en bout, IDEMIA Secure Transactions évalue les impacts à l'échelle des systèmes et aide à déterminer les activités de recherche nécessaires pour préparer les produits et les solutions digitales à être crypto-agiles.

En 2022 déjà, l'équipe cryptographie d'IDEMIA Secure Transactions dédiait un article à l'intégration de la cryptographie post-quantiques aux protocoles de paiement par carte bancaire.[5] Celui-ci a permis d'identifier les défis à relever pour maintenir le même niveau de fonctionnalité pour les paiements hors ligne qu'avec les protocoles EMV actuels. Avec cette approche de bout en bout, IDEMIA Secure Transactions s'est aussi récemment positionnée en pionnière des paiements hors ligne en monnaie numérique de banque centrale (CBDC) en faisant la démonstration d'une transaction résistante à l'ordinateur quantique utilisant une nouvelle solution cryptographique à clé publique.

Dans l'écosystème de l'Internet des Objets (IoT), IDEMIA Secure Transactions étudie les procédés de migration des appareils critiques qui ont une longue durée de vie, dont les ressources sont limitées et qui ne sont pas conçus pour être crypto-agiles. Dans le cadre de sa collaboration avec Telefónica et Quside, IDEMIA a démontré comment, dans un avenir proche, les capacités de crypto-agilité de l'eSIM pourraient être exploitées pour mettre à jour en toute sécurité le système d'exploitation d'un appareil afin d'offrir des services résistants à l'ordinateur quantique. Cette démonstration a montré comment effectuer de façon transparente la transition de la cryptographie classique à la cryptographie post-quantique, sans impact sur le matériel IoT. Ce partenariat est un premier pas vers la diffusion de nouveaux services cryptographiques auprès des développeurs IoT via la plateforme GSMA Open Gateway.

Ces preuves de concepts viennent en complément des contributions d'IDEMIA à la recherche mondiale et aux efforts de standardisation. En plus de sa participation aux initiatives du NIST, IDEMIA est également impliqué au sein de la GSMA, de l'ETSI, de GlobalPlatform et de l'alliance FIDO, ainsi qu'auprès de plusieurs organismes de standardisation et autres organisations en Inde dans les domaines des télécoms et de IoT. IDEMIA Secure Transactions a également mis en place des partenariats de recherche post-quantique en Europe avec l'INRIA et le CEA, ainsi qu'un partenariat de recherche stratégique avec l'Indian Institute of Technology Hyderabad (IIT Hyderabad).

Les enjeux de sécurité post-quantiques sont une réalité et il est urgent d'agir, tout en ayant conscience que l'agilité sera la clé pour maintenir la sécurité des transactions et des données dans le temps. Conscient de leur responsabilité, les acteurs de la sécurité sont mobilisés. La collaboration et l'investissement des entreprises qui dépendent de la cryptographie pour sécuriser leurs produits et leurs services est désormais cruciale pour développer et déployer les solutions cryptographiques de demain. Cette nouvelle ère de la cryptographie est aussi une opportunité formidable pour repenser et améliorer la sécurité des produits et services que nous utilisons tous les jours en prenant en compte de nouveaux enjeux, comme une meilleure protection de la vie privée par exemple.

---

[1] https://www.pwc.com/us/en/tech-effect/emerging-tech/emtech-survey.html
[2] https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
[3] Publications relatives à la sécurisation des implémentations de cryptographie post-quantique dans les environnements embarqués :
– ML-DSA (ex-Dilithium): https://dblp.org/rec/journals/tches/CoronGTZ23a.html , https://dblp.org/rec/journals/tches/CoronGLTZ24.html
– ML-KEM (ex-Kyber): https://dblp.org/rec/journals/tches/CoronGMZ22.html , https://dblp.org/rec/journals/tches/CoronGMZ23.html
– NTRU: https://dblp.org/rec/journals/tches/CoronGTZ23 ; https://dblp.org/rec/conf/cardis/BettaleEMRS22.html
[4] https://csrc.nist.gov/csrc/media/Presentations/2024/antrag-simplifying-and-improving-falcon/images-media/nguyen-antrag-pqc2024.pdf
[5] https://csrc.nist.gov/csrc/media/Events/2022/fourth-pqc-standardization-conference/documents/papers/post-quantum-protocols-for-banking-applications-pqc2022.pdf

---